AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A method ~~for preventing packet retransmissions during Internet Protocol security (IPsec) security association establishment~~ comprising:

intercepting a Transmission Control Protocol (TCP) connection request by an application;

negotiating for a security association;

establishing the security association; and

allowing the TCP connection request to proceed after the security association is established.

~~monitoring application socket requests;~~

~~requesting a Transmission Control Protocol (TCP) connection by an application;~~

~~determining if there is an active security association that exists to protect network flow associated with the connection request;~~

~~preventing the connection request from proceeding if no active security association exists to protect the network flow;~~

~~determining if a security policy exists for the network flow if no active security association exists to protect the network flow;~~

~~alerting a security association negotiation component to initiate negotiation for a security association based on the security policy if the security policy exists for the network flow; and~~

~~allowing the connection request to proceed if one of the active security association exists and the security association is established from the negotiation.~~

2. (Currently Amended) The method of ~~according to~~ claim 1, wherein the security association ~~negotiation component~~ comprises an Internet Key Exchange (IKE) component.

3. (Currently Amended) The method of ~~according to~~ claim 1, wherein ~~the active security association and~~ the security association is ~~are~~ based on ~~at least~~ one or more of the following:

a source Internet Protocol (IP) address;~~address,~~

a destination IP address;~~address,~~

a protocol;~~protocol,~~

a source port; ~~port,~~ and

a destination port.

4. (Currently Amended) The method of ~~according to~~ claim 3, wherein the protocol comprises one or more of the following:

TCP;~~TCP,~~

User Datagram Protocol (UDP);~~(UDP),~~

Internet Control Message Protocol (ICMP); ~~(ICMP),~~ and

Internet Group Management Protocol (IGMP).

5. (Currently Amended) The method of ~~according to~~ claim 1, further comprising:

determining if an active security association exists to protect network flow associated with the TCP connection request;

determining if a security policy exists for the network flow if no active security association exists to protect the network flow;

alerting a security association negotiation component to initiate negotiation for an alternative security association based on the security policy.

~~determining if the network flow can be allowed without a security association if no security policy exists for the network flow.~~

6. (Currently Amended) The method of ~~according to~~ claim 1, further comprising retrieving the security association from a database.

7. (Currently Amended) The method of ~~according to~~ claim 6, wherein the database contains mappings between network flow information and the security association~~associations~~.

8. (Currently Amended) The method of ~~according to~~ claim 7, wherein the network flow information comprises ~~at least~~ one or more of the following:

a source Internet Protocol (IP) address;~~address,~~

a destination IP address;~~address,~~

a protocol;~~protocol,~~

a source port; ~~port,~~ and

a destination port.

9. (Currently Amended) The method of ~~according to~~ claim 1, further comprising retrieving the security policy from the ~~a~~ database.

10. (Currently Amended) A method ~~for preventing packet retransmissions during Internet Protocol security (IPsec) security association establishment~~ comprising:

monitoring application socket requests;

requesting transmission of User Datagram Protocol (UDP) data on a socket by an application;

intercepting the transmission of the UDP data on the socket by the application;

determining if the socket has been associated with an active security association;

determining if there is a defined security association that may be used to protect network flow if the socket has not been associated with an active security association;

determining what security policy should be used when negotiating a security association for the network flow if there is no defined security association that may be used to protect the network flow;

~~preventing the UDP data from being sent if there is no defined security association that may be used to protect the network flow;~~

alerting a security association negotiation component to initiate negotiation for the security association if there is no defined security association that may be used to protect the network flow;

establishing the security association; and

allowing the UDP data to be sent in response to establishment of the security association.

11. (Currently Amended) The method of ~~according to~~ claim 10, wherein the security association negotiation component comprises an Internet Key Exchange (IKE) component.

12. (Currently Amended) The method of ~~according to~~ claim 10, comprising negotiating for the ~~a~~ security association using security parameters specified by the security ~~a~~ policy.

13. (Currently Amended) The method of ~~according to~~ claim 10, wherein the second determining comprises comparing filters with ~~at least~~ one or more of the following:

a source Internet Protocol (IP) address;~~address,~~

a destination IP address;~~address,~~

a protocol;~~protocol,~~

a source port; ~~port,~~ and

a destination port, wherein the destination port includes ~~the at least~~ one or more of the following

a source Internet Protocol (IP) address,

a destination IP address,

a protocol,

a source port, and

a destination port related to the network flow~~, the filters related to defined security associations~~.

14. (Currently Amended) The method of ~~according to~~ claim 13, wherein each filter comprises ~~comprising at least~~ one or more of the following:

a source Internet Protocol (IP) address;~~address,~~

a destination IP address; ~~address,~~

a protocol; ~~protocol,~~

a source port; ~~port,~~ and

a destination port.

15. (Currently Amended) The method of ~~according to~~ claim 13, wherein the security policy comprises at least one filter.

16. (Currently Amended) The method of ~~according to~~ claim 10, further comprising determining if the network flow can be allowed without the ~~a~~ security association if no security policy exists for the network flow.

17. (Currently Amended) A system ~~computing device for preventing packet retransmissions during Internet Protocol security (IPsec) security association establishment with a network unit, the device and network unit operably connected to a network, the computing device~~ comprising:

a network;

a network interceptor coupled with the network, the network interceptor to intercept a Transmission Control Protocol (TCP) connection request by an application; ~~monitoring an application's socket requests;~~

~~a security association database operably connected to the network interceptor, the security association database containing a mapping of network flow information to security association information;~~

~~a security policy database operably connected to the network interceptor, the security policy database containing policies that describe parameters that are to be used in a negotiation of a security association;~~

a security association negotiation component coupled with the network interceptor, the security association negotiation component ~~operably connected to the network interceptor, the security association negotiation component capable of negotiating~~ to negotiate a security association ~~with a network unit~~ and to establish the security association; and

the network interceptor to allow the TCP connection request to proceed after the security association is established.

~~an Internet Protocol security (IPsec) packet classifier, the IPsec packet classifier responsible for performing IPsec processing on incoming and outgoing packets, wherein the network interceptor insures that a security association is in place before allowing network traffic to flow between the application and the network unit.~~

18. (Currently Amended) The system of ~~device according to~~ claim 17, wherein the network flow information comprises ~~at least~~ one or more of the following:

Internet Protocol (IP) addresses;~~addresses,~~

a protocol;~~protocol,~~ and

ports.

19. (Currently Amended) The system of ~~device according to~~ claim 17, further comprising an Internet Protocol security (IPsec) packet classifier to be responsible for performing IPsec processing on incoming and outgoing packets, wherein the network interceptor insures that a security association is in place before allowing network traffic to flow between the application and the network unit ~~wherein the security association negotiation component comprises Internet Key Exchange (IKE)~~.

20. (Currently Amended) A machine-readable medium having stored thereon data representing sets of instructions which, when executed by a machine, cause the machine to: ~~An article comprising a storage medium having instructions stored therein, when~~

intercept a Transmission Control Protocol (TCP) connection request by an application;

negotiate for a security association;

establish the security association; and

allow the TCP connection request to proceed after the security association is established.

~~executed causes a computing device to perform:~~

~~monitoring application socket requests;~~

~~requesting a Transmission Control Protocol (TCP) connection by an application;~~

~~determining if there is an active security association that exists to protect network flow associated with the connection request;~~

~~preventing the connection request from proceeding if no active security association exists to protect the network flow;~~

~~determining if a security policy exists for the network flow if no active security association exists to protect the network flow;~~

~~alerting a security association negotiation component to initiate negotiation for a security association based on the security policy if the security policy exists for the network flow; and~~

~~allowing the connection request to proceed if one of the active security association exists and the security association is established from the negotiation.~~

21. (Currently Amended) The machine-readable medium of ~~The article according to~~ claim 20, wherein the security association negotiation component comprises an Internet Key Exchange (IKE) component.

22. (Currently Amended) The machine-readable medium of ~~The article according to~~ claim 20, further cause the machine to: ~~comprising negotiating for a security association using security parameters specified by a policy.~~

determine if an active security association exists to protect the network flow associated with the TCP connection request;

determine if a security policy exists for the network flow if no active security association exists to protect the network flow;

alert a security association negotiation component to initiate negotiation for an alternate security association based on the security policy if the security policy exists for the network flow.

23. (Currently Amended) The machine-readable medium of ~~The article according to~~ claim 20, wherein the active security association comprises ~~at least~~ one or more of the following:

a source Internet Protocol (IP);~~(IP),~~

a destination IP;~~IP,~~

a protocol;~~protocol,~~

a source port; ~~port,~~ and

a destination port.

24. (Currently Amended) A machine-readable medium having stored thereon data representing sets of instructions which, when executed by a machine, cause the machine to:~~An article comprising a storage medium having instructions stored therein, the instructions when executed causes a computing device to perform:~~

monitor ~~monitoring~~ application socket requests;

request ~~requesting~~ transmission of User Datagram Protocol (UDP) data on a socket by the application;

intercept the transmission of the UDP data on the socket by the application;

determine ~~determining~~ if the socket has been associated with an active security association;

determine ~~determining~~ if there is a defined security association that may be used to protect network flow if the socket has not been associated with an active security association;

determine ~~determining~~ what security policy should be used when negotiating a security association for the network flow if there is no defined security association that may be used to protect the network flow;

~~preventing the UDP data from being sent if there is no defined security association that may be used to protect the network flow;~~

alert ~~alerting~~ a security association negotiation component to initiate negotiation for the security association if there is no defined security association that may be used to protect the network flow;

establish ~~establishing~~ the security association; and

allow ~~allowing~~ the UDP data to be sent in response to establishment of the security association.

25. (Currently Amended) The machine-readable medium of ~~The article according to~~ claim 24, wherein the security association negotiation component comprises an Internet Key Exchange (IKE) component.

26. (Currently Amended) The machine-readable medium of ~~The article according to~~ claim 24, further cause the machine to negotiate ~~comprising negotiating~~ for the a security association using security parameters specified by a policy.

27. (Currently Amended) The machine-readable medium of ~~The article according to~~ claim 24, wherein the active security association comprises ~~at least~~ one or more of the following:

a source Internet Protocol (IP);~~(IP),~~

a destination IP;~~IP,~~

a protocol;~~protocol,~~

a source port; ~~port,~~ and

a destination port.

28-29. (Cancelled)